



**INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES
PÚBLICOS DO MUNICÍPIO DE TEÓFILO OTONI
SISPREV-TO
CNPJ: 05.110.612/0001-50**



PORTARIA Nº 45, DE 16 DE JULHO DE 2026

Aprova a Política de Segurança da Informação do SISPREV-TO e transforma a Comissão de Proteção de Dados em Comitê de Segurança da Informação e Proteção de Dados.

A DIRETORIA EXECUTIVA DO INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES PÚBLICOS DO MUNICÍPIO DE TEÓFILO OTONI - SISPREV-TO, no uso das atribuições legais que lhe são conferidas,

CONSIDERANDO a proteção de dados pessoais e o direito fundamental à proteção de dados, nos termos da Constituição Federal e da Lei Federal nº 13.709, de 14 de agosto de 2018;

CONSIDERANDO as disposições da Lei Federal nº 12.527, de 18 de novembro de 2011, e do Decreto Municipal nº 7.794, de 11 de abril de 2018;

CONSIDERANDO a necessidade de disciplinar a proteção das informações e a continuidade dos serviços previdenciários sob responsabilidade do SISPREV-TO;

CONSIDERANDO as diretrizes de governança, controles internos e segurança da informação.

RESOLVE:

Art. 1º Fica aprovada a Política de Segurança da Informação do SISPREV-TO, na forma do Anexo Único desta Portaria.

Art. 2º A Comissão de Proteção de Dados instituída pela Portaria SISPREV nº 18/2025 fica transformada em Comitê de Segurança da Informação e Proteção de Dados - CSIPD, composto pelos seguintes membros: I - Pericles de Oliveira Barbosa, Auxiliar Administrativo; II - Jardel Batista Carvalho Lopes, Diretor de Controle Interno; e III - Ketlyn Souza Batista, Diretoria Administrativa e Financeira.

Parágrafo único. O CSIPD exercerá as competências previstas nesta Portaria, na Política de Segurança da Informação e nos demais atos internos relacionados à proteção de dados e à segurança da informação.

Art. 3º Fica designado o servidor Pericles de Oliveira Barbosa como responsável pela execução das atividades técnicas de Tecnologia da Informação no âmbito do SISPREV-TO, sem criação de cargo ou unidade administrativa e sem prejuízo de suas atribuições funcionais.

Art. 4º A Política deverá ser divulgada aos servidores, estagiários, conselheiros, colaboradores e prestadores de serviços e publicada no endereço eletrônico institucional.

Art. 5º Os manuais, procedimentos, formulários e registros operacionais relacionados à segurança da informação serão mantidos em ambiente interno, com acesso compatível com sua finalidade e seu grau de sensibilidade.

Art. 6º Fica revogada a Portaria SISPREV nº 18/2025, preservados os atos praticados durante sua vigência.

Art. 7º Esta Portaria entra em vigor na data de sua publicação.

Teófilo Otoni/MG, 16 de julho de 2026.

GISELENE PEREIRA SILVA GOMES
Diretora-Presidente

KETLYN SOUZA BATISTA
Diretora Administrativo e Financeiro

RUTHNEIA LAUTON COSTA
Diretora de Previdência e Atuária



INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES
PÚBLICOS DO MUNICÍPIO DE TEÓFILO OTONI
SISPREV-TO
CNPJ: 05.110.612/0001-50



ANEXO ÚNICO À PORTARIA Nº 45/2026

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Documento

PSI/SISPREV-TO

Elaboração

Comitê de Segurança da Informação e Proteção de
Dados

Data

16 de julho de 2026

Teófilo Otoni/MG
2026



**INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES
PÚBLICOS DO MUNICÍPIO DE TEÓFILO OTONI
SISPREV-TO
CNPJ: 05.110.612/0001-50**



Controle do Documento

Título do documento	Política de Segurança da Informação do SISPREV-TO
Versão aprovada	1.0
Data da aprovação	16 de julho de 2026
Ato de aprovação	Portaria SISPREV nº 45, de 16 de julho de 2026
Unidade responsável	Comitê de Segurança da Informação e Proteção de Dados - CSIPD
Periodicidade de revisão	No máximo a cada 4 anos, ou antes quando necessário
Classificação de acesso	Documento público após aprovação
Responsável pela custódia	Comitê de Segurança da Informação e Proteção de Dados - CSIPD

Histórico de versões

Versão	Data	Descrição	Ato de aprovação
1.0	16/07/2026	Versão aprovada da Política de Segurança da Informação	Portaria SISPREV nº 45/2026

Documentos internos relacionados

- Manual e fluxograma de Controle de Acessos;
- Manual e fluxograma de Procedimentos de Contingência;
- Termo de Responsabilidade pelo Uso de Recursos de Tecnologia e Informação;
- Formulários e relatórios de concessão, alteração, revogação e auditoria de acessos;
- Registros de backup, testes de restauração, incidentes e capacitações;
- Política de Classificação da Informação e Tabela de Temporalidade e Destinação de Documentos, quando aprovadas.



**INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES
PÚBLICOS DO MUNICÍPIO DE TEÓFILO OTONI
SISPREV-TO
CNPJ: 05.110.612/0001-50**



SUMÁRIO

CAPÍTULO I-OBJETO, FINALIDADE E ABRANGÊNCIA.....	1
CAPÍTULO II-REFERÊNCIAS E DEFINIÇÕES	2
CAPÍTULO III-PRINCÍPIOS E DIRETRIZES GERAIS	3
CAPÍTULO IV-GOVERNANÇA E RESPONSABILIDADES.....	3
CAPÍTULO V-GESTÃO DE ATIVOS E DA INFORMAÇÃO	5
CAPÍTULO VI-SEGURANÇA RELACIONADA ÀS PESSOAS	5
CAPÍTULO VII-CONTROLE DE ACESSO FÍSICO	6
CAPÍTULO VIII-IDENTIDADE, SENHAS E ACESSO LÓGICO	6
CAPÍTULO IX-ESTAÇÕES, PROGRAMAS E ATUALIZAÇÕES	7
CAPÍTULO X-REDE, INTERNET E CONECTIVIDADE	8
CAPÍTULO XI-E-MAIL, MENSAGENS E REDES SOCIAIS	9
CAPÍTULO XII-ACESSO REMOTO, DISPOSITIVOS E TRABALHO EXTERNO	9
CAPÍTULO XIII-FORNECEDORES, PRESTADORES E SERVIÇOS EM NUVEM.....	10
CAPÍTULO XIV-REGISTROS, MONITORAMENTO E AUDITORIA	10
CAPÍTULO XV-BACKUP, RESTAURAÇÃO E CONTINUIDADE	11
CAPÍTULO XVI-GESTÃO DE INCIDENTES	12
CAPÍTULO XVII-DOCUMENTOS, MÍDIAS E DESCARTE.....	12
CAPÍTULO XVIII-CONSCIENTIZAÇÃO E CAPACITAÇÃO	13
CAPÍTULO XIX-CONFORMIDADE, EXEÇÕES E REVISÃO.....	14



**INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES
PÚBLICOS DO MUNICÍPIO DE TEÓFILO OTONI
SISPREV-TO
CNPJ: 05.110.612/0001-50**



CAPÍTULO I

OBJETO, FINALIDADE E ABRANGÊNCIA

Art. 1º Esta Política estabelece princípios, responsabilidades e controles para proteger as informações produzidas, recebidas, armazenadas, processadas, transmitidas ou custodiadas pelo SISPREV-TO, em meio físico ou digital.

Art. 2º São objetivos desta Política:

- I** - preservar a confidencialidade, a integridade, a disponibilidade, a autenticidade e a legalidade das informações;
- II** - proteger dados pessoais e informações previdenciárias contra acesso, uso, alteração, perda, destruição ou divulgação indevida;
- III** - assegurar continuidade, confiabilidade e recuperação dos serviços administrativos e previdenciários;
- IV** - definir deveres de dirigentes, servidores, estagiários, colaboradores e prestadores;
- V** - estabelecer controles proporcionais aos riscos e à estrutura do Instituto; e
- VI** - atender à legislação e aos requisitos de governança aplicáveis ao RPPS.

Art. 3º Esta Política aplica-se a dirigentes, conselheiros, servidores, estagiários, colaboradores, fornecedores e prestadores que acessem informações, sistemas, instalações, equipamentos ou recursos tecnológicos do SISPREV-TO.

Parágrafo único. A aplicação alcança atividades presenciais ou remotas, recursos próprios ou contratados e informações mantidas em sistemas locais, serviços em nuvem, correio eletrônico, mídias, documentos e arquivos físicos.

CAPÍTULO II

REFERÊNCIAS E DEFINIÇÕES

Art. 4º Esta Política fundamenta-se, especialmente, na Constituição Federal, nas Leis Federais nº 9.717/1998, nº 12.527/2011 e nº 13.709/2018, na Portaria MTP nº 1.467/2022 e alterações, no Decreto Municipal nº 7.794/2018.

Art. 5º Para fins desta Política, considera-se:

- I** - ativo de informação: dado, documento, conhecimento, sistema, equipamento, serviço, mídia, credencial ou ambiente que possua valor para o Instituto;
- II** - autenticidade: garantia de autoria, origem ou identidade atribuída à informação ou ao usuário;
- III** - confidencialidade: acesso à informação somente por pessoas autorizadas;
- IV** - disponibilidade: acesso à informação ou serviço por usuário autorizado quando necessário;
- V** - integridade: preservação da exatidão, completude e consistência da informação;
- VI** - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
- VII** - dado pessoal sensível: dado definido como sensível pela LGPD, inclusive referente à saúde, biometria e outras categorias legalmente protegidas;
- VIII** - credencial: identificação, senha, código, certificado, token ou outro meio usado para autenticação;
- IX** - conta privilegiada: conta com poderes de administração, configuração ou acesso ampliado;
- X** - incidente de segurança: evento confirmado ou suspeito que comprometa ou possa comprometer informação, sistema, equipamento ou serviço;
- XI** - log ou registro de evento: informação produzida por sistema ou procedimento para permitir rastreabilidade e auditoria;
- XII** - cópia de segurança ou backup: cópia destinada à recuperação da informação em caso de perda ou indisponibilidade;
- XIII** - restauração: processo de recuperação de informação a partir de backup;
- XIV** - RTO: tempo máximo pretendido para restabelecimento de um serviço;
- XV** - RPO: período máximo de perda de dados considerado aceitável para recuperação;
- XVI** - usuário: pessoa autorizada a acessar informação, sistema, equipamento ou instalação;

XVII - gestor da informação: autoridade ou responsável pela área capaz de autorizar acesso e definir regras de uso da informação;

XVIII - serviço em nuvem: recurso computacional ou sistema operado em infraestrutura externa e acessado por rede; e

XIX - menor privilégio: concessão apenas dos acessos indispensáveis e pelo tempo necessário.

CAPÍTULO III

PRINCÍPIOS E DIRETRIZES GERAIS

Art. 6º A segurança da informação observará os princípios da finalidade pública, necessidade, prevenção, responsabilização, transparência, continuidade, economicidade, proporcionalidade e melhoria contínua.

Art. 7º A proteção deverá acompanhar todo o ciclo de vida da informação, desde sua criação ou recebimento até a destinação final, considerando o suporte físico ou digital, o valor institucional, a sensibilidade e os prazos de guarda.

Art. 8º A publicidade constitui regra e o sigilo exceção, sem prejuízo da proteção de dados pessoais, das informações legalmente restritas e dos documentos cuja divulgação possa comprometer a segurança institucional.

Art. 9º Nenhuma medida de segurança deverá impedir, sem fundamento, o exercício das atribuições legais do SISPREV-TO, devendo os controles ser compatíveis com a realidade, os riscos e os recursos disponíveis.

CAPÍTULO IV

GOVERNANÇA E RESPONSABILIDADES

Art. 10. Compete à Diretoria-Executiva:

I - aprovar esta Política, suas revisões e os atos complementares de caráter institucional;

II - designar os membros do CSIPD e, quando cabível, o responsável pelas atividades técnicas de TI;

III - assegurar apoio administrativo e avaliar os recursos necessários à implantação dos controles;

IV - deliberar sobre riscos relevantes, medidas extraordinárias e comunicações institucionais; e

V - promover o alinhamento da segurança da informação com o planejamento e a governança do Instituto.

Art. 11. Compete ao Comitê de Segurança da Informação e Proteção de Dados - CSIPD:

I - definir e apoiar estratégias de implantação, manutenção e aprimoramento desta Política;

- II** - propor normas, projetos, capacitações, indicadores e planos de melhoria;
- III** - acompanhar riscos, incidentes, auditorias de acesso e testes de restauração;
- IV** - apoiar a classificação da informação e a definição de sua temporalidade;
- V** - orientar a divulgação das regras aos usuários e prestadores;
- VI** - registrar suas reuniões e acompanhar as providências deliberadas;
- VII** - emitir relatório anual das ações e resultados; e
- VIII** - propor revisão desta Política sempre que necessário.

Art. 12. Compete ao responsável pelas atividades técnicas de TI, dentro de sua designação e dos recursos disponíveis:

- I** - administrar ou acompanhar contas, permissões, equipamentos, rede, segurança e backups sob responsabilidade do Instituto;
- II** - executar controles técnicos, verificações, testes, registros e ações de recuperação;
- III** - comunicar riscos, falhas e incidentes à Diretoria e ao CSIPD;
- IV** - orientar usuários e acompanhar acessos técnicos de terceiros;
- V** - manter documentação técnica compatível com a continuidade das atividades; e
- VI** - propor melhorias, sem assumir isoladamente decisões administrativas, jurídicas, contratuais ou orçamentárias.

Art. 13. Compete aos dirigentes e gestores das áreas:

- I** - autorizar e revisar os acessos necessários às atribuições de suas equipes;
- II** - comunicar ingresso, movimentação, afastamento ou desligamento de pessoal;
- III** - orientar sobre a finalidade e a sensibilidade das informações tratadas;
- IV** - zelar pela guarda de documentos e pela adoção das medidas previstas nesta Política; e
- V** - informar riscos, falhas ou incidentes de que tenham conhecimento.

Art. 14. Todo usuário deverá utilizar os recursos institucionais de forma ética, legal e compatível com suas atribuições, proteger suas credenciais, armazenar documentos nos locais definidos e comunicar imediatamente qualquer suspeita de incidente.

Art. 15. O Controle Interno acompanhará, dentro de suas atribuições, a conformidade dos procedimentos e das evidências relacionadas a esta Política, sem substituir a responsabilidade dos gestores e executores de cada processo.

CAPÍTULO V

GESTÃO DE ATIVOS E DA INFORMAÇÃO

Art. 16. O SISPREV-TO manterá relação atualizada dos ativos relevantes, contendo, conforme aplicável, identificação, finalidade, localização, responsável, situação de uso e criticidade.

Art. 17. Os ativos deverão ser utilizados prioritariamente para atividades institucionais e protegidos contra dano, perda, uso indevido, alteração não autorizada e acesso por pessoa não habilitada.

Art. 18. Os documentos de trabalho que devam ser preservados e compartilhados serão armazenados nos repositórios institucionais definidos, evitando-se a manutenção exclusiva em estações locais, dispositivos pessoais ou canais não autorizados.

Art. 19. Informações previdenciárias, funcionais, financeiras, bancárias, jurídicas, atuariais e de saúde receberão proteção compatível com sua natureza e com a legislação aplicável.

Art. 20. A classificação e a temporalidade da informação serão disciplinadas em instrumentos específicos, com participação dos gestores das áreas, observadas a Lei de Acesso à Informação, a LGPD, as normas arquivísticas e as obrigações próprias dos RPPS.

Art. 21. A divulgação pública desta Política não alcança configurações, credenciais, diagramas detalhados, caminhos internos, inventários técnicos, vulnerabilidades ou procedimentos cuja exposição possa aumentar o risco à segurança.

CAPÍTULO VI

SEGURANÇA RELACIONADA ÀS PESSOAS

Art. 22. O acesso aos recursos institucionais será precedido de orientação compatível com a função e assinatura de Termo de Responsabilidade, inclusive por servidores, estagiários e colaboradores.

Art. 23. No ingresso ou na mudança de função, o gestor da área deverá informar os acessos necessários, evitando concessões baseadas apenas em conveniência, imitação de outro perfil ou solicitação sem justificativa funcional.

Art. 24. No afastamento, desligamento ou encerramento de contrato, os acessos deverão ser revisados ou bloqueados com a maior brevidade possível, preservando-se os documentos e registros institucionais.

Art. 25. Os deveres de confidencialidade e proteção da informação permanecem após o desligamento ou o término da relação com o SISPREV-TO.

Art. 26. O uso de equipamento, conta ou sistema por estagiário será compatível com suas atividades, supervisionado e limitado ao período do estágio.

CAPÍTULO VII

CONTROLE DE ACESSO FÍSICO

Art. 27. O acesso à sala que abriga servidores, equipamentos de rede, mídias de backup ou outros ativos críticos será limitado a pessoas autorizadas.

§ 1º Prestadores e visitantes somente poderão ingressar quando autorizados, acompanhados por servidor e registrados em formulário ou livro próprio.

§ 2º O registro deverá conter, no mínimo, data, horário, pessoa, empresa, finalidade, autorizador e responsável pelo acompanhamento.

Art. 28. A sala de equipamentos deverá possuir medidas compatíveis de proteção elétrica, climatização, prevenção de incêndio, organização, limpeza e redução de riscos ambientais.

Art. 29. Chaves, meios de abertura e autorizações de acesso serão mantidos sob controle, sendo proibida a entrega indiscriminada ou a permanência de pessoa não autorizada sem acompanhamento.

Art. 30. A movimentação, retirada, manutenção, transferência ou doação de equipamento deverá ser autorizada e registrada, observadas as regras patrimoniais e a remoção segura de dados.

CAPÍTULO VIII

IDENTIDADE, SENHAS E ACESSO LÓGICO

Art. 31. O acesso lógico será concedido com base em necessidade funcional, autorização do gestor e menor privilégio.

Art. 32. As contas deverão ser individuais, identificáveis e vinculadas ao respectivo usuário, sendo proibido compartilhar credenciais individuais ou utilizar conta pertencente a outra pessoa.

Art. 33. A criação, alteração, suspensão ou exclusão de acesso dependerá de solicitação ou ratificação por meio registrável, conforme procedimento interno, não sendo suficiente a comunicação exclusivamente verbal ou por mensagem instantânea.

Parágrafo único. Em situação urgente, a comunicação instantânea poderá iniciar o atendimento, desde que seja posteriormente formalizada.

Art. 34. A senha inicial será temporária e comunicada de maneira segura, devendo ser alterada pelo usuário no primeiro acesso sempre que o sistema permitir.

Art. 35. As senhas deverão ser de uso pessoal, suficientemente robustas e diferentes de combinações evidentes, sendo obrigatória sua alteração em caso de suspeita de exposição ou determinação administrativa.

Art. 36. A autenticação em dois fatores será habilitada quando disponível e tecnicamente viável, com prioridade para e-mail, serviços externos, redes sociais, contas privilegiadas e sistemas que tratem dados sensíveis.

Art. 37. Contas institucionais compartilhadas somente serão admitidas quando justificadas pela natureza do serviço e deverão possuir:

I - relação atualizada das pessoas autorizadas;

II - responsável por sua administração;

III - autenticação adicional, quando disponível;

IV - troca de senha quando houver mudança de equipe ou suspeita de comprometimento; e

V - restrição de uso à finalidade institucional.

Art. 38. Contas privilegiadas serão limitadas ao necessário, usadas apenas para tarefas administrativas e protegidas de forma distinta das contas comuns sempre que o ambiente permitir.

Art. 39. Credenciais de emergência terão guarda controlada, abertura ou uso registrado e alteração após utilização ou suspeita de exposição.

Art. 40. Os acessos lógicos serão auditados, no mínimo, semestralmente, mediante confronto entre usuários, vínculo, função, necessidade e permissões, com relatório das inconsistências e correções.

CAPÍTULO IX

ESTAÇÕES, PROGRAMAS E ATUALIZAÇÕES

Art. 41. As estações e servidores serão configurados com mecanismos de proteção disponíveis, incluindo controle administrativo, firewall, antimalware, atualizações de segurança e bloqueio de sessão, conforme compatibilidade técnica.

Art. 42. A instalação, remoção ou alteração de programa ou configuração administrativa dependerá de autorização e execução pelo responsável técnico ou pessoa por ele acompanhada.

Art. 43. É vedado ao usuário:

I – desativar, alterar, contornar ou tentar contornar mecanismos de segurança, incluindo antivírus, antimalware, firewall, bloqueio de sessão, autenticação, atualização e controle de acesso;

II – instalar, executar, copiar ou manter programa, aplicativo, extensão ou ferramenta sem autorização institucional;

III – criar, introduzir, transmitir ou disseminar intencionalmente vírus, código malicioso ou qualquer recurso destinado a causar dano, indisponibilidade, acesso indevido ou comprometimento de informações;

IV – explorar vulnerabilidades, obter acesso não autorizado ou facilitar o acesso de pessoa não autorizada a equipamento, sistema, conta, rede ou informação institucional;

V – ocultar incidente de segurança de que tenha conhecimento, destruir evidências ou dificultar sua apuração.

§ 1º Ao identificar ou suspeitar de vírus, programa malicioso, mensagem fraudulenta, comportamento anormal do equipamento ou acesso indevido, o usuário deverá interromper a atividade de risco, comunicar imediatamente o responsável pelas atividades técnicas de TI e seguir as orientações recebidas.

§ 2º O usuário não deverá, por iniciativa própria e sem orientação técnica, apagar arquivos, formatar o equipamento, reinstalar programas ou executar procedimentos que possam agravar o incidente ou eliminar evidências.

§ 3º A simples ocorrência de infecção, tentativa de fraude, recebimento de mensagem maliciosa ou outro incidente não caracteriza, por si só, descumprimento desta Política, devendo ser consideradas a conduta do usuário, o cumprimento das orientações recebidas e a comunicação tempestiva do fato.

Art. 44. Atualizações de sistema operacional, navegadores, programas e ferramentas de segurança serão aplicadas conforme disponibilidade, criticidade e compatibilidade, com registro quando houver adiamento relevante por risco operacional.

Art. 45. Dispositivos removíveis somente serão utilizados quando necessários, devendo ser verificados e protegidos contra perda, malware e acesso indevido.

CAPÍTULO X

REDE, INTERNET E CONECTIVIDADE

Art. 46. A rede destinada a visitantes deverá permanecer separada da rede interna e não permitirá acesso aos servidores, pastas compartilhadas, impressoras administrativas ou outros recursos institucionais.

Art. 47. As senhas das redes sem fio serão controladas pelo responsável técnico e alteradas quando necessário, sendo vedado fornecer credencial de rede interna a pessoa não autorizada.

Art. 48. O uso da internet deverá atender ao interesse institucional, respeitar a legislação e não comprometer a segurança, o desempenho da rede ou a imagem do SISPREV-TO.

Art. 49. Alterações de equipamentos de rede, regras de firewall, endereçamento ou conectividade dependerão de autorização e acompanhamento técnico.

Art. 50. Falhas de internet ou rede serão tratadas conforme o Plano de Contingência, com registro quando causarem impacto relevante aos serviços.

CAPÍTULO XI

E-MAIL, MENSAGENS E REDES SOCIAIS

Art. 51. O correio eletrônico e os canais de mensagem institucionais destinam-se às atividades do SISPREV-TO e deverão observar formalidade, finalidade, segurança e proteção de dados.

Art. 52. Antes do envio, o usuário deverá conferir destinatário, conteúdo, anexos e necessidade de compartilhamento, adotando cautela especial com dados pessoais, documentos previdenciários e informações restritas.

Art. 53. É vedado utilizar o e-mail institucional para correntes, conteúdo ilícito, manifestação político-partidária em nome do Instituto, envio deliberado de material ofensivo ou finalidade comercial estranha ao serviço.

Art. 54. As contas oficiais de redes sociais somente serão acessadas por responsáveis autorizados, com autenticação adicional quando disponível e revisão dos acessos sempre que houver mudança do prestador ou da equipe.

Art. 55. A contratação ou atuação de prestador de comunicação não lhe confere acesso a sistemas, documentos ou dados além do estritamente necessário à atividade autorizada.

Art. 56. A migração entre serviços de e-mail deverá preservar, na medida do possível, autenticidade, histórico, disponibilidade, segurança e continuidade das comunicações institucionais.

CAPÍTULO XII

ACESSO REMOTO, DISPOSITIVOS E TRABALHO EXTERNO

Art. 57. O acesso remoto por prestador será excepcional, autorizado para demanda específica, limitado ao tempo necessário e acompanhado por usuário responsável.

Parágrafo único. Não será mantida senha permanente para acesso remoto não assistido, salvo solução formalmente aprovada, tecnicamente justificada e sujeita a registro e revisão.

Art. 58. O usuário que utilizar notebook ou equipamento institucional fora da sede deverá protegê-lo contra furto, perda, visualização por terceiros e conexão a redes inseguras.

Art. 59. É vedado armazenar documentos institucionais em conta pessoal, dispositivo particular ou serviço de nuvem não autorizado, salvo situação excepcional formalmente aprovada e com medidas de proteção adequadas.

Art. 60. A perda, o furto ou a suspeita de comprometimento de equipamento, mídia ou credencial deverá ser comunicada imediatamente.

CAPÍTULO XIII

FORNECEDORES, PRESTADORES E SERVIÇOS EM NUVEM

Art. 61. Contratos ou instrumentos que envolvam acesso a dados, sistemas ou infraestrutura deverão prever, conforme o objeto, confidencialidade, proteção de dados, controle de acesso, continuidade, backup, comunicação de incidentes e devolução ou eliminação das informações.

Art. 62. O acesso de terceiro será concedido somente na extensão necessária, pelo menor prazo possível e, quando aplicável, por conta identificável e passível de registro.

Art. 63. Prestador que realize manutenção física em sala de equipamentos deverá ser autorizado, acompanhado e registrado, ainda que não acesse diretamente sistemas ou documentos.

Art. 64. A adoção ou renovação de serviço em nuvem considerará finalidade, dados tratados, disponibilidade, suporte, exportação das informações, encerramento do contrato e medidas de segurança oferecidas.

Art. 65. O gestor do contrato ou da demanda deverá informar ao CSIPD ou ao responsável técnico qualquer alteração relevante no serviço, no acesso do fornecedor ou no tratamento de informações.

CAPÍTULO XIV

REGISTROS, MONITORAMENTO E AUDITORIA

Art. 66. Os sistemas e procedimentos deverão produzir e preservar registros compatíveis com sua capacidade técnica e com a necessidade de rastreabilidade, respeitados os limites legais e a privacidade.

Art. 67. Registros de acesso, administração, backup, restauração, incidente e suporte serão acessados somente por pessoas autorizadas e utilizados para segurança, auditoria, continuidade ou apuração regular.

Art. 68. A ausência de ferramenta automatizada não dispensa a manutenção de registros administrativos mínimos por formulário, planilha, ata, relatório ou outro meio confiável.

Art. 69. Auditorias e verificações não deverão ser usadas para vigilância indiscriminada, devendo possuir finalidade institucional, proporcionalidade e acesso restrito aos resultados.

Art. 70. O CSIPD acompanhará indicadores mínimos de execução, incluindo capacitações realizadas, acessos revisados, backups verificados, restaurações testadas, incidentes registrados e providências pendentes.

CAPÍTULO XV

BACKUP, RESTAURAÇÃO E CONTINUIDADE

Art. 71. As informações institucionais relevantes serão incluídas em rotina de backup conforme criticidade, origem, capacidade técnica e necessidade de continuidade.

§ 1º Os documentos institucionais deverão ser armazenados na Pasta Central, nos sistemas oficiais ou em outro repositório expressamente autorizado, conforme a natureza da informação e as orientações institucionais.

§ 2º Arquivos mantidos exclusivamente na estação de trabalho poderão não estar abrangidos pela rotina institucional de backup.

§ 3º Os usuários serão orientados sobre os locais adequados de armazenamento, cabendo-lhes observar as orientações recebidas e comunicar eventual dificuldade.

§ 4º O disposto neste artigo não afasta a responsabilidade do SISPREV-TO pela adoção das medidas técnicas e administrativas de segurança compatíveis com sua estrutura e com os riscos existentes.

Art. 72. Os prazos de retenção das cópias de segurança dos dados digitais destinam-se à continuidade e à recuperação dos serviços e não substituem os prazos de guarda dos documentos estabelecidos na Tabela de Temporalidade e Destinação de Documentos.

Art. 73. Será mantida ao menos uma cópia desconectada do ambiente de origem e guardada em local fisicamente separado, com acesso restrito e proteção contra perda, dano e uso indevido.

Art. 74. O CSIPD avaliará anualmente a adoção de cópia externa segura ou solução equivalente capaz de reduzir o risco de perda simultânea do original e das cópias mantidas na sede.

Art. 75. A conclusão automática de uma rotina de backup não comprova, por si só, a possibilidade de recuperação, devendo os registros ser verificados e as falhas tratadas.

Art. 76. A restauração de amostra representativa será testada, no mínimo, semestralmente, em ambiente ou diretório isolado e sem sobrescrever dados de produção.

Parágrafo único. O teste registrará data, responsável, origem, arquivos ou sistema testado, resultado, tempo de recuperação e providências corretivas.

Art. 77. O Plano de Contingência definirá serviços essenciais, prioridades, RTO, RPO, responsáveis, substitutos, contatos, medidas de resposta e ordem de recuperação.

Art. 78. Os resultados de incidentes reais ou testes deverão ser utilizados para atualizar procedimentos, corrigir falhas e reavaliar prazos de recuperação.

CAPÍTULO XVI

GESTÃO DE INCIDENTES

Art. 79. Todo evento que possa comprometer informação, sistema, credencial, equipamento ou serviço deverá ser comunicado imediatamente ao responsável técnico, à chefia e, conforme a gravidade, ao CSIPD e à Diretoria-Executiva.

Art. 80. A resposta a incidente observará, conforme aplicável:

- I** - identificação e registro;
- II** - contenção e limitação do impacto;
- III** - preservação de registros e evidências;
- IV** - erradicação da causa e recuperação segura;
- V** - comunicação às partes competentes; e
- VI** - análise posterior e melhoria dos controles.

Art. 81. É vedada a divulgação externa de incidente por usuário sem autorização, ressalvadas comunicações obrigatórias e o exercício regular de direito perante autoridade competente.

Art. 82. Quando houver dados pessoais envolvidos, o SISPREV-TO avaliará a natureza, os titulares afetados, as medidas de proteção existentes, os riscos e a necessidade de comunicação à Autoridade Nacional de Proteção de Dados, aos titulares e a outros órgãos.

Art. 83. Mesmo quando não houver incidente conhecido, o CSIPD registrará anualmente a verificação realizada e manterá ações preventivas, testes e capacitações.

CAPÍTULO XVII

DOCUMENTOS, MÍDIAS E DESCARTE

Art. 84. Documentos físicos ou digitais contendo dados pessoais, previdenciários, financeiros, funcionais, jurídicos, atuariais ou de saúde serão acessados somente por pessoas cuja atividade exija seu conhecimento.

Art. 85. Quando o descarte estiver previamente autorizado nos termos do art. 87, os documentos que contenham informações pessoais ou restritas deverão ser fragmentados ou inutilizados de modo a impedir sua reconstrução.

Art. 86. Antes da transferência, doação, manutenção externa ou descarte de equipamento ou mídia, os dados serão removidos de forma segura, e a providência será registrada.

Art. 87. A eliminação de documentos institucionais, físicos ou digitais, somente ocorrerá após o cumprimento dos prazos e da destinação previstos na Tabela de Temporalidade e Destinação de Documentos, observadas as normas arquivísticas e as autorizações legalmente exigidas.

§ 1º É vedada a eliminação motivada exclusivamente por falta de espaço, conveniência administrativa ou redução de custos.

§ 2º Não poderão ser eliminados documentos relacionados a processo administrativo ou judicial, auditoria, fiscalização, investigação, requerimento de acesso à informação ou outra situação que exija sua preservação, ainda que tenha transcorrido o prazo previsto na Tabela de Temporalidade.

§ 3º A eliminação deverá ser previamente avaliada pela Comissão Permanente de Avaliação de Documentos — CPAD e documentada por meio dos instrumentos exigidos pelas normas aplicáveis, com autorização da instituição arquivística pública competente.

§ 4º A destruição autorizada será realizada de modo a impedir a reconstrução dos documentos e o acesso às informações neles contidas, com proteção dos dados pessoais e registro do procedimento.

§ 5º Até a aprovação da Tabela de Temporalidade e Destinação de Documentos e a confirmação ou constituição das instâncias arquivísticas competentes, fica vedada a eliminação de documentos institucionais, físicos ou digitais.

CAPÍTULO XVIII

CONSCIENTIZAÇÃO E CAPACITAÇÃO

Art. 88. O SISPREV-TO promoverá ação de conscientização ou capacitação em segurança da informação e proteção de dados, no mínimo, anualmente e sempre que houver mudança relevante de regra, risco ou tecnologia.

Art. 89. As ações considerarão os diferentes públicos, incluindo dirigentes, servidores, estagiários, conselheiros e prestadores, conforme sua atuação e exposição a riscos.

Art. 90. A comprovação será realizada por listas de presença, atas, certificados, materiais, fotografias, vídeos, publicações ou outros registros adequados.

Art. 91. Orientações breves e periódicas poderão ser divulgadas por e-mail, portal, reunião ou material educativo, complementando as capacitações formais.

CAPÍTULO XIX

CONFORMIDADE, EXCEÇÕES E REVISÃO

Art. 92. O CSIPD acompanhará anualmente o cumprimento desta Política e registrará não conformidades, recomendações, responsáveis e prazos de tratamento.

Art. 93. Exceção a controle previsto nesta Política dependerá de justificativa, avaliação do risco, prazo definido, aprovação da autoridade competente e, quando possível, adoção de medida compensatória.

Art. 94. O descumprimento desta Política será comunicado e apurado pela autoridade competente, em procedimento adequado à natureza do vínculo do envolvido, podendo resultar na aplicação das medidas previstas na legislação, no regime funcional, no termo de estágio, no contrato ou em outro instrumento aplicável.

§ 1º A apuração observará o contraditório, a ampla defesa, a competência da autoridade responsável e as demais garantias previstas na legislação.

§ 2º Na avaliação do fato serão considerados, entre outros elementos:

- I – a gravidade da conduta e o risco produzido;
- II – a existência de intenção, negligência, imprudência ou imperícia;
- III – os danos efetivamente causados;
- IV – a eventual reincidência;
- V – as orientações e capacitações anteriormente oferecidas;
- VI – a comunicação voluntária e tempestiva do fato; e
- VII – a colaboração do envolvido na contenção, apuração e correção do incidente.

§ 3º A comunicação de boa-fé de falha, vulnerabilidade, suspeita ou incidente não constitui infração, ainda que posteriormente o evento não seja confirmado.

§ 4º A responsabilidade administrativa ou contratual não afasta eventual responsabilidade civil ou penal, quando cabível, nos termos da legislação.

§ 5º Prestadores de serviços e demais terceiros estarão sujeitos às medidas previstas no contrato, termo de responsabilidade ou instrumento equivalente, incluindo suspensão ou revogação de acesso, sem prejuízo das demais providências cabíveis.



**INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES
PÚBLICOS DO MUNICÍPIO DE TEÓFILO OTONI
SISPREV-TO
CNPJ: 05.110.612/0001-50**



§ 6º. O SISPREV-TO poderá adotar imediatamente medidas técnicas de proteção, como bloqueio temporário de conta, suspensão de acesso, isolamento de equipamento, interrupção de conexão remota, preservação de registros e recolhimento preventivo de mídia.

§ 7º. As medidas previstas neste artigo possuem natureza preventiva e de contenção, não constituem penalidade nem antecipação de responsabilidade, devendo permanecer apenas pelo período necessário à proteção das informações e dos serviços.

Art. 95. Os casos omissos serão analisados pelo CSIPD e submetidos à Diretoria-Executiva quando envolverem decisão administrativa, jurídica, financeira, contratual ou institucional.

Art. 96. Esta Política será publicada no endereço eletrônico do SISPREV-TO, divulgada aos usuários e revisada quando houver alteração relevante e, obrigatoriamente, no máximo a cada quatro anos.

Art. 97. Os procedimentos técnicos complementares poderão ser atualizados sem republicação integral desta Política, desde que não contrariem suas diretrizes e sejam formalmente aprovados pela autoridade competente.

Art. 98. A implantação inicial dos controles, formulários e registros previstos nesta Política será realizada progressivamente, sob acompanhamento do CSIPD, observados os seguintes prazos, contados da publicação da Portaria que a aprova:

- I - aplicação imediata às novas concessões, alterações e revogações de acesso, aos incidentes, aos acessos de terceiros e aos demais eventos ocorridos após a publicação;
- II - até 90 dias para o levantamento inicial dos ativos, a regularização dos registros existentes e a adoção dos instrumentos previstos nos Apêndices;
- III - até 180 dias para a realização da primeira auditoria de acessos lógicos e do primeiro teste formal de restauração; e
- IV - até 12 meses para a primeira execução das atividades de periodicidade anual, observadas, posteriormente, as periodicidades previstas nesta Política.

APÊNDICE A - DOCUMENTOS E REGISTROS MÍNIMOS

O quadro abaixo orienta a produção das evidências necessárias à implantação e ao acompanhamento da Política. A periodicidade poderá ser reduzida quando houver risco, incidente ou mudança relevante.

Documento ou registro	Responsável principal	Periodicidade mínima	Evidência
Ato de aprovação da PSI	Diretoria-Executiva	Na aprovação e revisão	Portaria e publicação
Composição do CSIPD	Diretoria-Executiva	Quando houver alteração	Portaria
Reuniões do CSIPD	CSIPD	Conforme calendário e necessidade	Ata ou relatório
Relatório anual do CSIPD	CSIPD	Anual	Relatório assinado
Termos de responsabilidade	Gestores / área administrativa	No ingresso ou concessão de acesso	Termo assinado
Solicitações de acesso	Gestor da área	A cada evento	Formulário, e-mail ou processo
Auditoria de acessos	Responsável técnico / gestores	Semestral	Relatório e correções
Controle de terceiros na sala técnica	Acompanhante	A cada acesso	Livro ou formulário
Verificação de backup	Responsável técnico	Conforme rotina	Log, relatório ou planilha
Teste de restauração	Responsável técnico / CSIPD	Semestral	Relatório do teste
Registro de incidente	Responsável pelo tratamento	A cada evento	Formulário ou relatório
Capacitação e conscientização	CSIPD / Diretoria	Anual e quando necessário	Lista, ata, certificado ou mídia
Inventário de ativos	Responsável técnico / Patrimônio	Anual e quando houver mudança	Planilha ou sistema
Revisão da PSI	CSIPD / Diretoria	Até 4 anos	Nova versão e ato de aprovação

APÊNDICE B - CONTEÚDO MÍNIMO DO REGISTRO DE INCIDENTE

- Número ou identificação do registro;
- data e horário de identificação;
- nome de quem comunicou e área envolvida;
- descrição objetiva do evento ou suspeita;
- informações, equipamentos, sistemas ou serviços afetados;
- dados pessoais possivelmente envolvidos e categorias de titulares;
- medidas imediatas de contenção;
- prestadores ou autoridades acionados;
- tempo de indisponibilidade e de recuperação;
- causa conhecida ou provável;
- resultado, impacto e pendências;
- medidas corretivas e responsáveis;
- avaliação sobre comunicação à ANPD, aos titulares ou a outros órgãos; e
- aprovação ou ciência da Diretoria e do CSIPD, conforme gravidade.

Observação: o registro não deve incluir senhas, chaves de acesso ou outros segredos técnicos. Informações sensíveis da investigação deverão ser mantidas em anexo restrito.

APÊNDICE C - ROTEIRO DA AUDITORIA DE ACESSO LÓGICO

- Obter relação atual de servidores, estagiários, prestadores e respectivos vínculos;
- listar usuários do domínio e dos principais sistemas;
- conferir contas sem responsável identificado, inativas ou de pessoas desligadas;
- comparar permissões com a função e a área de atuação;
- verificar contas privilegiadas e acessos de terceiros;
- revisar usuários das contas institucionais compartilhadas;
- verificar autenticação em dois fatores onde prevista;
- registrar inconsistências, providências, responsáveis e prazos;
- confirmar bloqueios, exclusões ou ajustes realizados; e
- submeter o relatório ao CSIPD e aos gestores das áreas.

APÊNDICE D - CONTEÚDO MÍNIMO DO TESTE DE RESTAURAÇÃO

Campo	Conteúdo esperado
Identificação	Número, data, responsável e participantes.
Origem	Rotina, mídia ou conjunto de backup utilizado.
Escopo	Arquivos, pastas, configurações ou sistema selecionado para o teste.
Ambiente	Pasta ou ambiente isolado, sem substituição de dados de produção.
Critério de sucesso	Abertura, integridade, completude e legibilidade dos itens restaurados.
Tempo	Horário de início, término e duração da recuperação.
Resultado	Sucesso, sucesso parcial ou falha, com justificativa.
Correções	Providências, responsáveis e prazo quando houver falha.
Validação	Ciência do responsável técnico e do CSIPD.

REFERÊNCIAS NORMATIVAS

- Constituição da República Federativa do Brasil de 1988;
- Lei Federal nº 9.717, de 27 de novembro de 1998;
- Lei Federal nº 12.527, de 18 de novembro de 2011 - Lei de Acesso à Informação;
- Lei Federal nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais;
- Portaria MTP nº 1.467, de 2 de junho de 2022, e alterações;
- Decreto Municipal nº 7.794, de 11 de abril de 2018;

Teófilo Otoni/MG, 16 de julho de 2026.